

Deterministic Compressed Sensing Matrices from Multiplicative Character Sequences

Nam Yul Yu

Department of Electrical Engineering, Lakehead University
Thunder Bay, ON, CANADA
Email: nam.yu@lakeheadu.ca

Abstract—Compressed sensing is a novel technique where one can recover sparse signals from the undersampled measurements. In this paper, a $K \times N$ measurement matrix for compressed sensing is deterministically constructed via multiplicative character sequences. Precisely, a constant multiple of a cyclic shift of an M -ary power residue or Sidelnikov sequence is arranged as a column vector of the matrix, through modulating a primitive M -th root of unity. The Weil bound is then used to show that the matrix has asymptotically optimal coherence for large K and M , and to present a sufficient condition on the sparsity level for unique sparse solution. Also, the restricted isometry property (RIP) is statistically studied for the deterministic matrix. Numerical results show that the deterministic compressed sensing matrix guarantees reliable matching pursuit recovery performance for both noiseless and noisy measurements.

Index Terms—Compressed sensing, multiplicative characters, power residue sequences, restricted isometry property, Sidelnikov sequences, Weil bound.

I. INTRODUCTION

Compressed sensing (or compressive sampling) is a novel and emerging technology with a variety of applications in imaging, data compression, and communications. In compressed sensing, one can recover sparse signals of high dimension from few measurements that were believed to be incomplete. Mathematically, measuring an N -dimensional signal $\mathbf{x} \in \mathbb{R}^N$ with a $K \times N$ measurement matrix \mathbf{A} produces a K -dimensional vector $\mathbf{y} = \mathbf{A}\mathbf{x}$ in compressed sensing, where $K < N$. In recovering \mathbf{x} , it seems impossible to solve K linear equations with N indeterminates by basic linear algebra. However, imposing an additional requirement that \mathbf{x} is s -sparse or the number of nonzero entries in \mathbf{x} is at most s , one can recover \mathbf{x} exactly with high probability by solving the l_1 -minimization problem, which is computationally tractable.

Many research activities have been triggered on theory and practice of compressed sensing since Donoho [1], and Candes, Romberg, and Tao [2][3] published their marvelous theoretical works. The efforts revealed that a measurement matrix \mathbf{A} plays a crucial role in recovery of s -sparse signals. In particular, Candes and Tao [3] presented the *restricted isometry property (RIP)*, a sufficient condition for the matrix to guarantee sparse recovery. A *random* matrix has been widely studied for satisfying the RIP, where the entries are generated by a probability distribution such as the Gaussian or Bernoulli process, or from randomly chosen partial Fourier ensembles.

Although a random matrix has many theoretical benefits [4], it has the drawbacks [5] of high complexity, large storage, and low efficiency in its practical implementation. As an alternative, we may consider a *deterministic* matrix, where well known codes and sequences have been employed for the construction, e.g., chirp sequences [6], Kerdock and Delsarte-Goethals codes [7], second order Reed-Muller codes [8], and dual BCH codes [9]. Other techniques for deterministic construction, based on finite fields, representation theory, additive characters, and cyclic difference sets, can be found in [10]–[14]. Although it is difficult to check the RIP and the theoretical recovery bounds are worse than that of a random matrix [4], deterministic matrices guarantee reliable recovery performance in a statistical sense, allowing fast processing and low complexity.

To enjoy the benefits of deterministic construction, this paper presents how to construct a $K \times N$ measurement matrix for compressed sensing via *multiplicative character sequences*. Precisely, we construct the matrix where a constant multiple of a cyclic shift of an M -ary power residue or Sidelnikov sequence of length K is arranged as a column vector, through modulating a primitive M -th root of unity. The Weil bound is then used to show that the matrix has asymptotically optimal coherence for large K and M , and to present the theoretical bound on the sparsity level for unique sparse solution. The RIP of the matrix is also analyzed through the eigenvalue statistics of the Gram matrices as in [5] and [6]. Through numerical results, we observe that the matching pursuit recovery for our deterministic matrices provides stable and reliable performance in recovering sparse signals with or without measurement noise.

The rest of this paper is organized as follows. In Section II, we describe the background for understanding this work. Section III presents the main contribution of this paper by constructing compressed sensing matrices from multiplicative character sequences, and studying the properties on sparse recovery. In Section IV, numerical results of the recovery performance are given for noiseless and noisy measurements. Concluding remarks will be given in Section V.

II. PRELIMINARIES

The following notations will be used throughout this paper.

- $\omega_M = e^{j\frac{2\pi}{M}}$ is a primitive M -th root of unity, where $j = \sqrt{-1}$.
- $\mathbb{F}_q = \text{GF}(q)$ is the finite field with q elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ denotes the multiplicative group of \mathbb{F}_q .
- $\mathbb{F}_q[x]$ is the polynomial ring over \mathbb{F}_q , where each coefficient of $f(x) \in \mathbb{F}_q[x]$ is an element of \mathbb{F}_q .
- For x in \mathbb{F}_q , a *logarithm* over \mathbb{F}_q is defined by

$$\log_\alpha x = \begin{cases} t, & \text{if } x = \alpha^t, 0 \leq t \leq q-2, \\ 0, & \text{if } x = 0 \end{cases}$$

where α is a primitive element in \mathbb{F}_q .

A. Multiplicative characters

Definition 1: Let α be a primitive element in \mathbb{F}_q and M a divisor of $q-1$, i.e., $M \mid q-1$. We define a *multiplicative character* of \mathbb{F}_q of order M by

$$\psi(x) = \exp\left(j\frac{2\pi \log_\alpha x}{M}\right), \quad x \in \mathbb{F}_q \quad (1)$$

where $\psi(0) = 1$ by the definition of the log operation.

For the original definition of multiplicative characters, see [15]. In (1), note that $\psi(0) = 1$, which contradicts the conventional assumption in [15]. In this paper, however, we keep the assumption of $\psi(0) = 1$ to maintain the definition of (1), which is convenient for this work. Throughout this paper, $\psi(x)$ may be denoted as ψ if the context is clear.

The Weil bound [16] gives an upper bound on the magnitude of multiplicative character sums. We introduce the refined version (Corollary 1 in [17]) supporting the assumption $\psi(0) = 1$.

Proposition 1: [17] Let $f_1(x), \dots, f_l(x)$ be l monic and irreducible polynomials in $\mathbb{F}_q[x]$ which have positive degrees d_1, \dots, d_l , respectively. Let d be the number of distinct roots of $f(x) = \prod_{i=1}^l f_i(x)$ in its splitting field over \mathbb{F}_q . Then, $d \leq \sum_{i=1}^l d_i$, where the equality is achieved if $f_i(x)$'s are distinct. Let ψ_1, \dots, ψ_l be multiplicative characters of \mathbb{F}_q . Assume that the product character $\prod_{i=1}^l \psi_i(f_i(x))$ is nontrivial, i.e., $\prod_{i=1}^l \psi_i(f_i(x)) \neq 1$ for some $x \in \mathbb{F}_q$. Let e_i be the number of distinct roots in \mathbb{F}_q of $f_i(x)$, where $i = 1, \dots, l$. If $\psi_i(0) = 1$ for each i , then for every $a_i \in \mathbb{F}_q^*$, $i = 1, \dots, l$, we have

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \leq (d-1) \sqrt{q} + \sum_{i=1}^l e_i. \quad (2)$$

In Proposition 1, d in (2) can be replaced by $\sum_{i=1}^l d_i$, since $d \leq \sum_{i=1}^l d_i$. The replacement allows us to have no need of distinguishing whether or not the polynomials are distinct, which is useful for this work.

B. Restricted isometry property

The restricted isometry property (RIP) [3] presents a sufficient condition for a measurement matrix \mathbf{A} to guarantee unique sparse recovery.

Definition 2: The restricted isometry constant δ_s of a $K \times N$ matrix \mathbf{A} is defined as the smallest number such that

$$(1 - \delta_s) \|\mathbf{x}\|_{l_2}^2 \leq \|\mathbf{A}\mathbf{x}\|_{l_2}^2 \leq (1 + \delta_s) \|\mathbf{x}\|_{l_2}^2$$

holds for all s -sparse vectors $\mathbf{x} \in \mathbb{R}^N$, where $\|\mathbf{x}\|_{l_2}^2 = \sum_{n=0}^{N-1} |x_n|^2$ with $\mathbf{x} = (x_0, \dots, x_{N-1})^T$.

We say that \mathbf{A} obeys the RIP of order s if δ_s is reasonably small, not close to 1. In fact, the RIP requires that all subsets of s columns taken from the measurement matrix should be *nearly orthogonal* [18]. Indeed, Candes [19] asserted that if $\delta_{2s} < 1$, a unique s -sparse solution is guaranteed by l_0 -minimization, which is however a hard combinatorial problem.

A tractable approach for sparse recovery is to solve the l_1 -minimization, i.e., to find a solution of $\min_{\tilde{\mathbf{x}} \in \mathbb{R}^N} \|\tilde{\mathbf{x}}\|_{l_1}$ subject to $\mathbf{A}\tilde{\mathbf{x}} = \mathbf{y}$, where $\|\tilde{\mathbf{x}}\|_{l_1} = \sum_{i=0}^{N-1} |\tilde{x}_i|$. In addition, greedy algorithms [20] have been also proposed for sparse signal recovery, including matching pursuit (MP) [21], orthogonal matching pursuit (OMP) [22], and CoSaMP [23]. If a deterministic measurement matrix is used, its structure may be exploited to develop a reconstruction algorithm for sparse signal recovery, providing fast processing and low complexity [6][8].

C. Coherence and redundancy

In compressed sensing, a $K \times N$ deterministic matrix \mathbf{A} is associated with two geometric quantities, *coherence* and *redundancy* [24]. The coherence μ is defined by

$$\mu = \max_{0 \leq l \neq m \leq N-1} |\mathbf{a}_l^H \cdot \mathbf{a}_m|$$

where \mathbf{a}_* denotes a column vector of \mathbf{A} with $\|\mathbf{a}_*\|_{l_2} = 1$, and \mathbf{a}_*^H is its conjugate transpose. In fact, the coherence is a measure of mutual orthogonality among columns, and the small coherence is desired for good sparse recovery [4]. In general, the coherence is lower bounded by

$$\mu \geq \sqrt{\frac{N-K}{K(N-1)}}$$

which is called the *Welch bound* [25].

The redundancy, on the other hand, is defined as $\rho = \|\mathbf{A}\|^2$, where $\|\cdot\|$ denotes the spectral norm of \mathbf{A} , or the largest singular value of \mathbf{A} . We have $\rho \geq N/K$, where the equality holds if and only if \mathbf{A} is a *tight frame* [26]. For unique sparse recovery, it is also desired that \mathbf{A} should be a tight frame with the smallest redundancy [26].

III. COMPRESSED SENSING MATRICES FROM MULTIPLICATIVE CHARACTER SEQUENCES

Sidelnikov [27] introduced two types of polyphase sequences with low periodic autocorrelation. In what follows, we define the sequences by logarithm and construct compressed sensing matrices using the sequences.

A. Construction from power residue sequences

Definition 3: Let p be an odd prime and M a divisor of $p-1$, i.e., $M \mid p-1$. Let α be a primitive root modulo p . An M -ary power residue sequence $\mathbf{r} = \{r(k) \mid 0 \leq k \leq p-1\}$ of period p is defined by

$$r(k) \equiv \log_\alpha k \pmod{M}. \quad (3)$$

By (1) and (3), the modulated sequence of $r(k)$ is represented by

$$\omega_M^{r(k)} = \psi(k), \quad 0 \leq k \leq p-1$$

where $\psi(0) = 1$.

Employing the power residue sequence, we construct a compressed sensing matrix.

Construction 1: Let $\mathbf{r} = \{r(k) \mid 0 \leq k \leq p-1\}$ be an M -ary power residue sequence of period p , where $M > 2$. Let $K = p$ and $N = (M-1)K$. In a $K \times N$ matrix \mathbf{A} , set each column index as $n = (c-1)K + b$, where $b \equiv n \pmod{K}$ and $c = \lfloor \frac{n}{K} \rfloor + 1$ for $0 \leq b \leq p-1$ and $1 \leq c \leq M-1$. Then, we construct a $K \times N$ compressed sensing matrix \mathbf{A} where each entry is given by

$$a_{k,n} = \frac{1}{\sqrt{K}} \omega_M^{cr(k+b)} = \frac{1}{\sqrt{K}} \psi((k+b)^c), \\ 0 \leq k \leq K-1, \quad 0 \leq n \leq N-1$$

where $k+b$ is computed modulo p .

Theorem 1: For the $K \times N$ matrix \mathbf{A} in Construction 1, the coherence is given by

$$\mu = \max_{0 \leq n_1 \neq n_2 \leq N-1} |\mathbf{a}_{n_1}^H \cdot \mathbf{a}_{n_2}| = \frac{\sqrt{K}+2}{K} \quad (4)$$

where \mathbf{a}_* denotes a column vector of \mathbf{A} . In particular, if K and M are large, the coherence is asymptotically optimal achieving the equality of the Welch bound.

Proof. Consider the column indices of $n_1 = (c_1-1)K + b_1$ and $n_2 = (c_2-1)K + b_2$, where $n_1 \neq n_2$. Set $x = k \in \mathbb{F}_p$. Then, the Weil bound in Proposition 1 gives an upper bound on the magnitude of the inner product of a pair of columns in \mathbf{A} , i.e.,

$$|\mathbf{a}_{n_1}^H \cdot \mathbf{a}_{n_2}| = \frac{1}{K} \left| \sum_{x \in \mathbb{F}_p} \psi((x+b_1)^{-c_1}) \cdot \psi((x+b_2)^{c_2}) \right| \\ = \frac{1}{K} \left| \sum_{x \in \mathbb{F}_p} \psi_1(x+b_1) \psi_2(x+b_2) \right| \\ \leq \frac{\sqrt{K}+2}{K}$$

where $\psi_1 = \psi^{-c_1}$ and $\psi_2 = \psi^{c_2}$. Therefore, the coherence in (4) is immediate. For large K , $\mu \approx \frac{1}{\sqrt{K}}$ from (4). Also, the equality of the Welch bound is $\sqrt{\frac{N-K}{K(N-1)}} = \sqrt{\frac{M-2}{(M-1)K-1}} \approx \frac{1}{\sqrt{K}}$ for large M . Thus, the coherence asymptotically achieves the equality of the Welch bound for large K and M . \square

Tropp [20] revealed that $(2s-1)\mu < 1$ ensures s -sparse signal recovery by basis pursuit (BP) and orthogonal matching pursuit (OMP). With the sufficient condition, Gribonval and Vanderghelynst [28] further showed that matching pursuit (MP) also derives a unique solution with exponential convergence. Using the results, Theorem 2 provides a sufficient condition for the matrix \mathbf{A} in Construction 1.

Theorem 2: For the matrix \mathbf{A} in Construction 1, a unique s -sparse solution is guaranteed by l_1 -minimization or greedy algorithms if

$$s < \frac{1}{2} \left(\frac{K}{\sqrt{K}+2} + 1 \right).$$

Proof. The upper bound on the sparsity level is straightforward from the coherence $\mu = \frac{\sqrt{K}+2}{K}$ and the Tropp's condition $(2s-1)\mu < 1$. \square

B. Construction from Sidelnikov sequences

Definition 4: Let α be a primitive element in the finite field \mathbb{F}_{p^m} and M a divisor of p^m-1 , where p is prime and m is a positive integer. An M -ary Sidelnikov sequence $\mathbf{s} = \{s(k) \mid 0 \leq k \leq p^m-2\}$ of period p^m-1 is defined by

$$s(k) \equiv \log_\alpha(\alpha^k + 1) \pmod{M}. \quad (5)$$

By (1) and (5), the modulated sequence of $s(k)$ is represented by

$$\omega_M^{s(k)} = \psi(\alpha^k + 1), \quad 0 \leq k \leq p^m-2$$

where $\psi(0) = 1$.

Construction 2: Let $\mathbf{s} = \{s(k) \mid 0 \leq k \leq p^m-2\}$ be an M -ary Sidelnikov sequence of period p^m-1 , where $M > 2$. Let $K = p^m-1$ and $N = (M-1)K$. In a $K \times N$ matrix $\hat{\mathbf{A}}$, set each column index as $n = (c-1)K + b$, where $b \equiv n \pmod{K}$ and $c = \lfloor \frac{n}{K} \rfloor + 1$ for $0 \leq b \leq p^m-2$ and $1 \leq c \leq M-1$. Then, we construct a $K \times N$ compressed sensing matrix $\hat{\mathbf{A}}$ where each entry is given by

$$\hat{a}_{k,n} = \frac{1}{\sqrt{K}} \omega_M^{cs(k+b)} = \frac{1}{\sqrt{K}} \psi((\lambda \alpha^k + 1)^c), \\ 0 \leq k \leq K-1, \quad 0 \leq n \leq N-1$$

where $\lambda = \alpha^b \in \mathbb{F}_{p^m}^*$ and $k+b$ is computed modulo p^m-1 .

Theorem 3: For the $K \times N$ matrix $\hat{\mathbf{A}}$ in Construction 2, the coherence is given by

$$\mu = \max_{0 \leq n_1 \neq n_2 \leq N-1} |\hat{\mathbf{a}}_{n_1}^H \cdot \hat{\mathbf{a}}_{n_2}| = \frac{\sqrt{K+1}+3}{K}. \quad (6)$$

where $\hat{\mathbf{a}}_*$ denotes a column vector of $\hat{\mathbf{A}}$. For large K and M , the coherence is asymptotically optimal achieving the equality of the Welch bound.

Proof. Consider the column indices of $n_1 = (c_1-1)K + b_1$ and $n_2 = (c_2-1)K + b_2$, where $n_1 \neq n_2$. Let $\lambda_1 = \alpha^{b_1}$, $\lambda_2 = \alpha^{b_2}$, and $x = \alpha^k \in \mathbb{F}_{p^m}^*$. Using the Weil bound in

TABLE I
THE SPECTRAL NORMS OF \mathbf{A} AND $\hat{\mathbf{A}}$

(K, N, M)	$\ \mathbf{A}\ $	$\sqrt{N/K}$	(K, N, M)	$\ \hat{\mathbf{A}}\ $	$\sqrt{N/K}$
(43, 1763, 42)	6.6282	6.4031	(26, 650, 26)	5.0990	5
(59, 3363, 58)	7.7431	7.5498	(48, 2256, 48)	6.9282	6.8557
(67, 4355, 66)	8.2439	8.0623	(80, 6320, 80)	8.9443	8.8882
(83, 6723, 82)	9.1635	9	(124, 15252, 124)	11.1355	11.0905
(97, 9215, 96)	9.8982	9.7468	(168, 28056, 168)	12.9615	12.9228

Proposition 1, the inner product of a pair of columns in \mathbf{A} has the magnitude bounded by

$$\begin{aligned}
|\hat{\mathbf{a}}_{n_1}^H \cdot \hat{\mathbf{a}}_{n_2}| &= \frac{1}{K} \left| \sum_{x \in \mathbb{F}_{p^m}^*} \psi((\lambda_1 x + 1)^{-c_1}) \cdot \psi((\lambda_2 x + 1)^{c_2}) \right| \\
&= \frac{1}{K} \left| \sum_{x \in \mathbb{F}_{p^m}^*} \psi_1(\lambda_1 x + 1) \psi_2(\lambda_2 x + 1) \right| \\
&= \frac{1}{K} \left(\left| \sum_{x \in \mathbb{F}_{p^m}^*} \psi_1(\lambda_1 x + 1) \psi_2(\lambda_2 x + 1) \right| + 1 \right) \\
&\leq \frac{\sqrt{K+1} + 3}{K}
\end{aligned}$$

where $\psi_1 = \psi^{-c_1}$ and $\psi_2 = \psi^{c_2}$. Therefore, the coherence in (6) is immediate. Similar to the approach made in the proof of Theorem 1, the coherence asymptotically achieves the equality of the Welch bound for large K and M . \square

With the coherence and the Tropp's sufficient condition [20], the sparsity bound of $\hat{\mathbf{A}}$ is straightforward.

Theorem 4: For the matrix $\hat{\mathbf{A}}$ in Construction 2, a unique s -sparse solution is guaranteed by l_1 -minimization or greedy algorithms if

$$s < \frac{1}{2} \left(\frac{K}{\sqrt{K+1} + 3} + 1 \right).$$

Remark 1: In Constructions 1 and 2, it is easily checked that a pair of rows in the matrix \mathbf{A} (or $\hat{\mathbf{A}}$) may not be mutually orthogonal, which implies that \mathbf{A} (or $\hat{\mathbf{A}}$) is not a tight frame. However, numerical data reveals that their spectral norms are nearly optimal, as shown in Table I for some values of K , N , and M .

Remark 2: In Constructions 1 and 2, each column vector of \mathbf{A} (or $\hat{\mathbf{A}}$) is equivalent to a modulated sequence of a constant multiple of a cyclic shift of a power residue or Sidelnikov sequence. Therefore, only a single base sequence is required for the implementation of the compressed sensing matrix, which allows low complexity and storage. In particular, if m is even, we can generate a Sidelnikov sequence of period $p^m - 1$ using an efficient linear feedback shift register (LFSR) [29], which further reduces the implementation complexity. Moreover, the alphabet size M of the matrix is variable depending

on the signal dimension N , as N is a function of M in the constructions. In summary, we can efficiently implement a variety of compressed sensing matrices with various alphabet and column sizes from multiplicative character sequences.

C. RIP analysis

For statistical RIP analysis, we chose $(K, N, M) = (47, 2115, 46)$ for power residue sensing matrix \mathbf{A} , and $(K, N, M) = (48, 2256, 48)$ for Sidelnikov sensing matrix $\hat{\mathbf{A}}$, respectively. For each matrix, taking its submatrix with randomly chosen s columns, we then measured the condition number, defined as the ratio of the largest singular value of each submatrix to the smallest.

In Figure 1, we measured the means and standard deviations of the condition numbers of \mathbf{A}_s , $\hat{\mathbf{A}}_s$, and \mathbf{G}_s , where \mathbf{A}_s and $\hat{\mathbf{A}}_s$ are the submatrices of s columns randomly chosen from \mathbf{A} and $\hat{\mathbf{A}}$, respectively, while \mathbf{G}_s is a $K \times s$ Gaussian random matrix with $K = 48$. The statistics were measured over total 10,000 condition numbers, where each matrix is newly chosen at each instance. Each entry of the Gaussian matrix \mathbf{G}_s is independently sampled from the Gaussian distribution of zero mean and variance $\frac{1}{K}$, and each column vector is then normalized such that it has unit l_2 -norm.

Note that the singular values of \mathbf{A}_s (or $\hat{\mathbf{A}}_s$) are the square roots of eigenvalues of the Gram matrix $\mathbf{A}_s^H \mathbf{A}_s$ (or $\hat{\mathbf{A}}_s^H \hat{\mathbf{A}}_s$). Then, the condition numbers should be as small as possible for sparse signal recovery, since the RIP requires that the Gram matrix should have all the eigenvalues in an interval $[1 - \delta_s, 1 + \delta_s]$ with reasonably small δ_s [4]. From this point of view, we see that the power residue and Sidelnikov sensing matrices show better statistics of condition numbers than the Gaussian random matrix in Figure 1. We made similar observations in the statistics of power residue sensing matrix with $(K, N, M) = (127, 15875, 126)$ and Sidelnikov matrix with $(K, N, M) = (124, 15252, 124)$. This convinces us that \mathbf{A} and $\hat{\mathbf{A}}$ in Constructions 1 and 2 are suitable for compressed sensing in a statistical sense.

IV. RECOVERY PERFORMANCE

A. Recovery from noiseless data

Figure 2 shows numerical results on successful recovery rates of s -sparse signals measured by power residue sensing matrix \mathbf{A} with $(K, N, M) = (47, 2115, 46)$, and Sidelnikov matrix $\hat{\mathbf{A}}$ with $(K, N, M) = (48, 2256, 48)$, respectively, where total 2000 sample vectors were tested for each sparsity

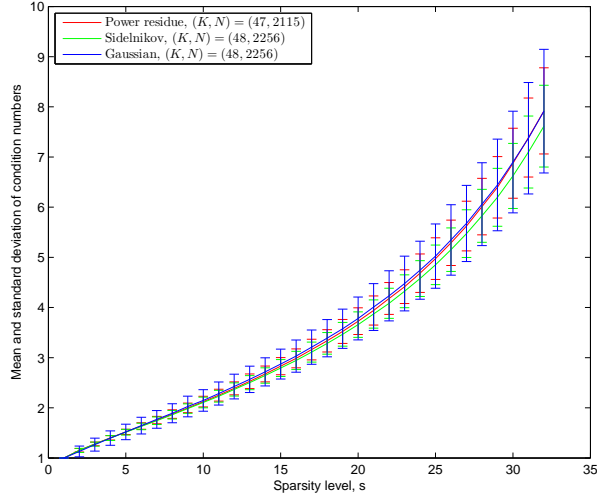


Fig. 1. Condition number statistics of the Gram matrices of power residue, Sidelnikov, and Gaussian random sensing matrices.

level. For comparison, the figure also displays the rate for 48×2256 randomly chosen partial Fourier matrix, where a new matrix is used at each instance of an s -sparse signal, in order to obtain the average rate. For all the matrices, the matching pursuit recovery with 100 iterations has been applied for the reconstruction of sparse signals. Each nonzero entry of an s -sparse signal \mathbf{x} has the magnitude of 1, where its position and sign are chosen uniformly at random. A success is declared in the reconstruction if the squared error is reasonably small for the estimate $\hat{\mathbf{x}}$, i.e., $\|\mathbf{x} - \hat{\mathbf{x}}\|_{l_2}^2 < 10^{-4}$.

In the figure, we observe that if $s \leq 3$, more than 99% of s -sparse signals are successfully recovered for the power residue sensing matrix, which statistically verifies the sufficient condition in Theorem 2. Similarly, the sufficient condition of the Sidelnikov sensing matrix in Theorem 4 is also verified for $s \leq 2$. In fact, the figure reveals that the sufficient conditions are somewhat pessimistic, since the actual recovery performance is fairly good even for high sparsity levels. For example, both sensing matrices guarantee more than 95% successful recovery rates if $s \leq 4$. Furthermore, the matrices present better recovery performance than randomly chosen partial Fourier matrices. We made similar observations in the recovery performance of other power residue $((K, N, M) = (127, 15875, 126))$ and Sidelnikov $((K, N, M) = (124, 15252, 124))$ sensing matrices.

B. Recovery from noisy data

In practice, a measured signal \mathbf{y} contains noise, i.e., $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{z}$, where $\mathbf{z} \in \mathbb{C}^K$ denotes a K -dimensional complex vector of noise. Thus, a compressed sensing matrix must be robust to the measurement noise for stable and noise resilient recovery. Figure 3 displays the matching pursuit recovery performance of various compressed sensing matrices in the presence of noise. The matrix parameters and the sparse signal

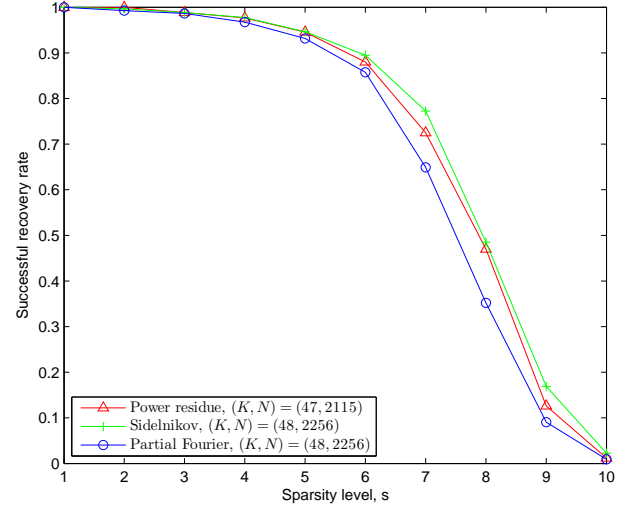


Fig. 2. Successful recovery rates for power residue, Sidelnikov, and partial Fourier sensing matrices for noiseless sparse signals.

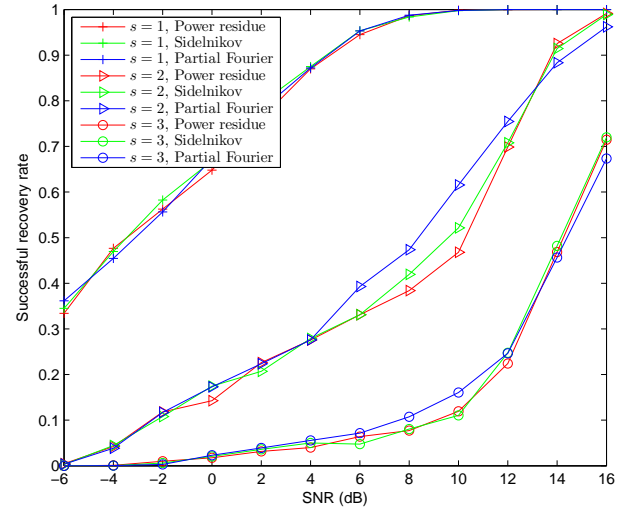


Fig. 3. Successful recovery rates for power residue, Sidelnikov, and partial Fourier sensing matrices in the presence of noise. $((K, N) = (47, 2115))$ for power residue and $((K, N) = (48, 2256))$ for the others

generation are identical to those of noiseless case. In the figure, \mathbf{x} is s -sparse for $s = 1, 2, 3$, and the signal-to-noise ratio (SNR) is defined by $\text{SNR} = \frac{\|\mathbf{A}\mathbf{x}\|_{l_2}^2}{K\sigma_z^2}$, where each element of \mathbf{z} is an independent and identically distributed (i.i.d.) complex Gaussian random process with zero mean and variance σ_z^2 . In noisy recovery, a success is declared if $\|\mathbf{x} - \hat{\mathbf{x}}\|_{l_2}^2 < 10^{-2}$ after 100 iterations. From Figure 3, we observe that the recovery performance is stable and robust against noise corruption at sufficiently high SNR, which is similar to that of randomly chosen partial Fourier matrices.

V. CONCLUSION

This paper has presented how to deterministically construct a $K \times N$ measurement matrix for compressed sensing via multiplicative character sequences. We showed that the matrices from M -ary power residue and Sidelnikov sequences have asymptotically optimal coherence for large K and M . We also presented the sufficient conditions on the sparsity level for unique sparse solution. Furthermore, the RIP of the matrices has been statistically analyzed, where we observed that they have better condition number statistics than Gaussian random matrices. Numerical results revealed that the compressed sensing matrices show stable and reliable performance in matching pursuit recovery for sparse signals with or without measurement noise. Finally, we would like to mention that the compressed sensing matrices can be implemented with small storage and low complexity, as each column vector is equivalently generated by a constant multiple of a cyclic shift of a single base power residue or Sidelnikov sequence.

REFERENCES

- [1] D. L. Donoho, "Compressed Sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289-1306, Apr. 2006.
- [2] E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489-509, Feb. 2006.
- [3] E. J. Candes and T. Tao, "Near-optimal signal recovery from random projections: universal encoding strategies," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406-5425, Dec. 2006.
- [4] H. Rauhut, "Compressive sensing and structured random matrices," *preprint*, May 2010.
- [5] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 358-374, Apr. 2010.
- [6] L. Applebaum, S. D. Howard, S. Searle, and R. Calderbank, "Chirp sensing codes: deterministic compressed sensing measurements for fast recovery," *Appl. and Comput. Harmon. Anal.*, vol. 26, pp. 283-290, 2009.
- [7] R. Calderbank, S. Howard, and S. Jafarpour, "A sublinear algorithm for sparse reconstruction with l_2/l_2 recovery guarantees," *arXiv:0806.3799v2 [cs.IT]*, Oct. 2009.
- [8] S. Howard, R. Calderbank, and S. Searle, "A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes," *Conference on Information Systems and Sciences (CISS)*, Princeton, NJ, Mar. 2008.
- [9] N. Ailon and E. Liberty, "Fast dimension reduction using Rademacher series on dual BCH codes," *Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 215-224, Jan. 2008.
- [10] R. A. DeVore, "Deterministic constructions of compressed sensing matrices," *Journal of Complexity*, vol. 28, pp. 918-925, 2007.
- [11] S. Gurevich, R. Hadani, and N. Sochen, "On some deterministic dictionaries supporting sparsity," *Journal of Fourier Analysis and Applications*, To appear.
- [12] Z. Xu, "Deterministic sampling of sparse trigonometric polynomials," *arXiv:1006.2221v1 [math.NA]*, June 2010.
- [13] N. Y. Yu, "Deterministic compressed sensing matrices from additive character sequences," *arXiv:1010.0011v1 [cs.IT]*, Oct. 2010.
- [14] N. Y. Yu, "Deterministic construction of partial Fourier compressed sensing matrices via cyclic difference sets," *arXiv:1008.0885v1 [cs.IT]*, Aug. 2010.
- [15] R. Lidl and H. Niederreiter, *Finite Fields*, in *Encyclopedia of Mathematics and Its Applications*, vol. 20, Cambridge University Press, 1997.
- [16] A. Weil, *Basic Number Theory*, 3rd. Ed., Springer-Verlag, 1974.
- [17] N. Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," *IEEE Trans. Inf. Theory*, To appear. Also available at CACR 2009-25, *CACR Technical Report*, University of Waterloo, 2009.
- [18] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Sig. Proc. Mag.*, pp. 21-30, Mar. 2008.
- [19] E. J. Candes, "The restricted isometry property and its implications for compressed sensing," *Academie des sciences*, Feb. 2008.
- [20] J. A. Tropp, "Greed is good: algorithmic results for sparse approximation," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2231-2242, Oct. 2004.
- [21] S. Mallat and Z. Zhang, "Matching pursuits with time-frequency dictionaries," *IEEE Trans. Signal Processing*, vol. 41, pp. 3397-3415, Dec. 1993.
- [22] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655-4666, Dec. 2007.
- [23] D. Needell and J. A. Tropp, "CoSaMP: Iterative signal recovery from incomplete and inaccurate samples," *Appl. and Comput. Harmon. Anal.*, vol. 26, pp. 301-321, 2009.
- [24] J. A. Tropp, "The sparsity gap: uncertainty principle proportional to dimension," *Conference on Information Systems and Sciences (CISS)*, Princeton, NJ, Mar. 2010.
- [25] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 3, pp. 397-399, May 1974.
- [26] R. Calderbank and S. Jafarpour, "Reed Muller sensing matrices and the LASSO," *arXiv:1004.4949v1 [cs.IT]*, Apr. 2010.
- [27] V. M. Sidelnikov, "Some k -valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, pp. 12-16, 1969.
- [28] R. Gribonval and P. Vandergheynst, "On the exponential convergence of matching pursuits in quasi-incoherent dictionaries," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 255-261, Jan. 2006.
- [29] N. Y. Yu and G. Gong, "New construction of M -ary sequence families with low correlation from the structure of Sidelnikov sequences," *IEEE Trans. on Inf. Theory*, vol. 56, no. 8, pp. 4061-4070, Aug. 2010.